VULNERABLE BY DESIGN: MITIGATING DESIGN FLAWS IN HARDWARE AND SOFTWARE

Konoth, R.K.

2020

document version
Publisher's PDF, also known as Version of record

Samenvatting

Ontwerpfouten en implementatiefouten zijn twee verschillende soorten beveiligingsgebreken. Ontwerpfouten zijn fouten die zich voordoen in de ontwerpfase, terwijl implementatiefouten fouten zijn die zich voordoen in de implementatiefase van de productontwikkelingscyclus. Helaas is de huidige focus van de systeembeveiligingsgemeenschap meer gericht op veelvoorkomende implementatiefouten dan op ontwerpfouten, ook al vormen ontwerpfouten 50% van de beveiligingsgebreken.

Om de gebruiksvriendelijkheid en prestaties te verbeteren, introduceren zowel applicatieontwikkelaars als platformverkopers voortdurend nieuwe functies (zoals *synchronisatiefuncties*), en vaak resulteert een dergelijke wens tot verhoogde gebruiksvriendelijkheid/prestatie in een schending van de principes van veilig ontwerp. Dit is de reden waarom de meeste ontwerpfouten zichtbaar zijn als producteigenschappen maar toch niet gezien worden. Aanvallers kunnen profiteren van de onbedoelde gevolgen van dergelijke functies om het hele systeem in gevaar te brengen. Dit is een andere manier van misbruik in vergelijking met typische manieren om geheugenfouten te misbruiken. Om deze reden is het normaal gesproken moeilijk om dergelijke fouten te ontdekken, en in vergelijking met een implementatiefout is het complex om een ontwerpfout te herstellen. Dit vereist vaak oplossingen die voor elke aanval uniek zijn.

In deze dissertatie onderzoeken wij ontwerpfouten die kunnen voorkomen op het software- en hardwareniveau van computersystemen, en de cyberbedreigingen die daaruit voortvloeien. We bouwen nieuwe softwarematige computerbeveiliging om te beschermen tegen de geïdentificeerde cyberbedreigingen en bespreken de kosten die ermee gepaard gaan. Bovendien wordt dit onderzoek verbreed door na te gaan of de huidige verzameling van ontwerpprincipes uitgebreid genoeg is om de huidige cyberdreigingen te voorkomen. We bereiken dit doel door een diepgaande analyse uit te voeren van een nieuwe cyberaanval, *cryptojacking* genaamd, die het algemeen aanvaarde veiligheidsmodel van van-